

I, Robert Erdely, hereby depose and state the following:

1. I am currently a Detective with the Computer Crime Unit of the Indiana County Pennsylvania's Detective Bureau. I was previously employed as the supervisor for the Pennsylvania State Police Computer Crime Unit until I retired in 2012. The Computer Crime Unit is responsible for investigations of crimes which occur on the Internet including the distribution of child exploitation material through peer-to-peer networks.
2. I have 23 years of experience in law enforcement, with 16 of these years specializing in computer crime. For 12 of these years and at the present time I provide instruction to law enforcement officers on the skills necessary to conduct online investigations and computer forensic examinations, including investigations involving Peer-to-Peer file sharing networks.
3. I was certified in 1999 as an Electronic Evidence Collection Specialist by the International Association of Computer Investigative Specialists, in 2007 as a Certified Forensic computer Examiner by the International Association of Investigative Specialists, and in 2009 as an Access Data Certified Forensic Examiner. I hold numerous other certifications in information technology for systems from Microsoft, Cisco, CompTIA, and ISC2.
4. I assisted in the development of the *RoundUp eMule* program which was designed to be used for the investigation of sharing child exploitation material through peer-to-peer file sharing eDonkey/KAD networks. I currently instruct other law enforcement officers how to utilize the *RoundUp eMule* program through classes sponsored by the Internet Crimes Against Children Task Force, a federally funded task force comprised of local, state and federal law enforcement agencies dedicated to investigating the online trafficking of child pornography and online child exploitation cases.

Peer-to-Peer File Sharing on the eMule Network

5. Peer-to-Peer (P2P) file sharing programs allow users to directly connect to other users on the same P2P network to transfer through the Internet. Many of these programs are available for free to Internet users including eMule. Any files stored in a P2P user's shared directory are available for download by any other user of the same file sharing network. When a user starts the eMule program it publishes the files shared on the eDonkey network to indexes that are stored on eDonkey servers and/or KAD ("eDonkey/KAD network" herein). Both the eDonkey and KAD servers act as an index which is searchable by other users of this file sharing network. For each file being shared, the user publishes the following information to the indexing server: file name; file size; hash value; user's IP address and port. The indexing server stores this information and makes it available to other users on the network seeking similar files.
6. eMule does not use or rely on supernodes as an index; rather, a different file sharing network known as Ares uses supernodes as an indexer. The Swedish pirate bay discussed by defendant in his Motion to Suppress acts as an index on the bittorrent file sharing network, which is not part of the eMule file sharing network.
7. The file sharing network is designed to allow users to query the indexing servers (eDonkey and KAD) by either keyword or hash value of files being shared on the network. The indexing server then responds with a list of file names that match the keywords queried allowing the user to select the file(s) desired to download. The indexing server then provides the user a list of IP addresses and port numbers that are sharing the desired file through a secondary search which happens automatically by the program. This secondary search is where eMule will search by hash value for IP addresses sharing the file selected for download. The user's software then initiates a multi-source download directly from those IP

addresses and ports. No portions of the file are stored on or received by the indexing servers.

8. Hash values are the result of a numerical algorithm reflecting the details contained within a file. Different algorithms result in different hash values which uniquely identify the file and are often referred to as digital signatures. The eDonkey/KAD network uses a variation of the MD4 algorithm called the eD2k MD4 to calculate hash values of files offered to the public in shared folders. These hash values are made available to the public on the eMule and KAD indexing servers. Although the hashing algorithm is a modified version of the MD4 hashing algorithm, a free hash calculator is available on the internet called "SlavaSoft HashCalc". Additionally, any user of the publically available eMule program has the ability to let eMule hash a file, then view that file hash.
9. To initiate a file download, the user's computer conducts a handshake or data exchange with the sharing computer where both computers exchange the version number of the P2P software in use, and a nickname the user has specified in the eMule program. If no nickname is specified, a default nickname is typically used. Additionally a unique identifier called a "client user hash" value, and their public keys are also often exchanged. The eMule client only writes this data exchanged to a file used by eMule called "clients.met" if data is transferred. If the two computers conduct a handshake but then do not transmit additional data, the eMule system will not choose to store this data. Law Enforcement cannot force this data to be stored by the eMule program.
10. If the index server reports only one computer sharing the desired file, then the eMule client can download the complete file from that one source. Although a download from a single IP address is possible, the use of any of the freely available IP filtering programs could ensure

that a transfer of a file was achieved from only one sharing IP address running the eMule Program.

11. The indexing servers assign users ID numbers. Generally the indexing servers assign low IDs if the user is using a firewall. A user can be designated a low ID at one point in time and high ID at a different time. Other factors also can effect whether a user has a low ID or a high ID. The fact that a user is designated a low ID at a certain time does not indicate that his eMule program will always have a low ID. In researching the Law Enforcement's search results in the investigation of this IP on the eDonkey/KAD network, I found instances of the IP address in question being assigned a low id. I reviewed the download attempts made in this investigation and in my opinion, the failed download attempt is not due to a low ID. The *Roundup eMule* program was able to connect to the suspect computer and exchange information and therefore was not a low ID. In reviewing the case details I have concluded that the failed download is most likely due to encrypted drives which held the files not being available. Encrypted drives are only visible if the user passes login credentials. When an encrypted drive is in this state, it is considered to be mounted. When the user dismounts the drive, it is now protected with a password and the contents are not visible. If eMule was running and a drive is dismounted, the download would fail. The download would also fail if the file was moved from the shared folder. In this case, the files referenced in the affidavit were found in the encrypted drives. For example, the file having the Sha1 Hash "4A67D0742E2F7620E2B1F43B0A6F15E4FF97CC0E" was found on numerous storage devices seized from the defendant.
12. eMule utilizes a priority system to assign order in a line of users waiting to download any file in order to encourage uploading of files. Users providing a great number of files available

for sharing can result in a higher priority to download files. This priority system will continuously update the users ranking and can vary at different points in time.

Roundup version of eMule

13. The *Roundup eMule* program is the version of the P2P file sharing program used by law enforcement to identify child exploitation files being shared on the eDonkey/KAD P2P network. Law enforcement has had a great deal of difficulty in the past. Prior to the development of *Roundup eMule* and similar investigative tools, Law Enforcement had great difficulty in identifying those using P2P users who were distributing child exploitation materials as Law Enforcement cannot share such contraband nor could they access the networks without allowing themselves to receive and potentially distribute this child exploitation material. Therefore, it was virtually impossible for Law Enforcement to identify those using P2P networks to distribute, receive, and possess child exploitation files. *Roundup eMule* is an important tool for law enforcement in identifying the IP address of these involved in the distribution and receipt of child exploitation materials.
14. The *Roundup eMule* program only enables law enforcement officers to query the indexing servers located on the P2P network. Once these indexing servers respond with a list of files being shared with the public through eMule, the law enforcement employee can then select a file to investigate further. In accordance with the eDonkey protocol, the indexing server then provides the *RoundUp eMule* program the IP address and port reported to be sharing that file. Just as any other eMule user, the RoundUp emule program then requests a copy of the desired file from directly from an IP address. RoundUp emule cannot access any files or user information not made available to the public either through the user's shared folder or on the indexing servers.

15. The *RoundUp eMule* program contains features not present in the file sharing program available for the public. For example, the RoundUp program provides investigators the unique hash values for known child pornography images and videos. By comparing these hash values to the hash values of the images shared by other users through the P2P network, law enforcement officers can more quickly determine which shared files contain child exploitation material.
16. There is a list of ED2K MD4 hash values for files related to child exploitation included with *Roundup eMule*. Once a matching eD2k MD4 hash value is identified on the eDonkey/KAD network, law enforcement can also identify this image with its SHA1 hash. If any person possesses a file, they can calculate any hash value. Some examples of hash values are the ED2K MD4, MD4, MD5, SHA1 and SHA256. An investigator would want to calculate either the MD5 or SHA1 when requesting assistance from the National Center for Missing and Exploited Children (NCMEC) for NCMEC keeps track of images and movies using both of these hashing algorithms. Once calculated, Law Enforcement can submit the MD5 or SHA1 to determine if the victim depicted in the file has been previously identified by Law Enforcement.
17. All images downloaded using the *RoundUp eMule* program are entirely downloaded from one IP address. The *RoundUp eMule* program does not obtain portions of the downloaded image from several different IP addresses, but instead only obtains the entire image from one IP address.
18. The *RoundUp eMule* program provides the investigator the ability to appear as if he/she is sharing files with the public. This is referred to as honeypotting or fake file sharing. When an investigator chooses to use this feature in the *RoundUp eMule* program, the investigator can select from files which appear to be child exploitation material yet do not constitute

child exploitation material. These files would need to be placed in the shared folder. Other P2P users can see the file names and can request a download, however, the *RoundUp eMule* program will never allow any portion of the file to be downloaded. This information is part of the computer program *Roundup eMule*, its manual and protocols, and its technical specifications. This information is law enforcement sensitive as disclosure of these items could be used by offenders to escape detection. Additionally, in researching the Law Enforcement's search results in this case on the eDonkey/KAD network, it is apparent that this feature was not used in this investigation.

19. The *RoundUp eMule* program utilizes the same handshake feature the standard eMule program conducts when it initiates a download request from another P2P user. The *RoundUp eMule* program stores all information it receives during this handshake, regardless of whether any additional data is transferred after the handshake. If the P2P user's computer chooses to store the data exchanged during this handshaking function, then the unique ID used by the *RoundUp eMule* program may be located on the computer which the eMule program was running on during a subsequent forensic exam. For this reason, the RoundUp eMule makes a note of the data exchanged to and received from the eMule program under investigation. The *RoundUp eMule* program does not and cannot force the P2P user's computer to store any information. This is sometimes referred to as a tagging feature but this is simply a detailed logging of the communication between the investigative computer and the suspect computer. RoundUp eMule cannot force any data to be written to an eMule program. RoundUp eMule cannot send files to an eMule program because eMule is a program designed to download files from other eDonkey compatible programs. It cannot put files which have not been requested by the eMule program. Since *RoundUp eMule* is incapable of sharing files, it is impossible that *RoundUp eMule* can put any files

onto any computer system regardless of whether a request was received for a file or not.


The *RoundUp eMule* program also incorporates the approximation of an IP Address's physical location provided through a company "Maxmind". Maxmind has a publically available database where any internet user can search the approximate location of an IP address; that database is located at Maxmind.com. Law Enforcement uses this approximate location in order to identify suspect computers sharing files in their primary jurisdiction. Since this is only an approximate location, Law Enforcement relies on the Internet Service Providers identification of the subscriber using the IP address at the date(s) and time(s) of the violation.

20. Defendant states that *RoundUp eMule* "manipulates" an offender's computer, causing it to "return data that would not normally be available to the public." This is untrue. *RoundUp eMule* had no impact upon the data returned by Feldman's, nor any other offender's, computer. Instead, *RoundUp eMule* obtains data about files offered for distribution precisely as any other P2P program does, by seeking out files that an offender has widely broadcast to a public P2P network that he is making available to download. While *RoundUp eMule* searches the eMule network, it does not gather this information directly from defendant's computer itself, but rather, from the eDonkey/KAD network. This is information which the eMule program published. If the eMule program was not sharing the file, the file details would not be published to the eDonkey/KAD network. The eDonkey/KAD network collects this type of information from a variety of P2P users, and then shares that information with all users of the P2P platform.


21. Defendant states that generating hash values of child exploitation files is a function proprietary to *RoundUp eMule*. This is untrue. File hashing is a widely-used mathematical

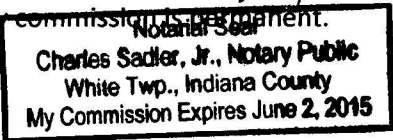
process that is integral to the operation of public P2P file sharing networks, and which can duplicated by the defense expert.

22. The FBI sought the assistance of MITRE Corporation to conduct validation testing on the *RoundUp eMule* program. This testing confirmed that *RoundUp eMule* conducts single source downloads and does not share files even if files are located in the shared folder. MITRE Corporation is a public interest company that applies systems engineering and advanced technology in research and development centers. The MITRE website reports over 7,000 employees.
23. The law enforcement privilege protects the source code of the *RoundUp eMule* computer program from compelled disclosure to defendants and the public because such disclosure would jeopardize this investigative technique as well as ongoing investigations by enabling these offenders to detect and circumvent the efforts of law enforcement. The source code is locked meaning it is not even available to law enforcement agents who utilize the tool. I do not even have the source code. The source code has only been made available to the FBI for validation testing.
24. By disclosing this source code of the *RoundUp eMule* program to the defendant, the hash values of known child pornography images and the results of other law enforcement queries could be compromised. Criminals would be able to circumvent law enforcement efforts while continuing to distribute the child abuse and exploitation material to the public.


Detective Robert Erdely
Indiana County District Attorney's Office

Subscribed and sworn to me this
24 day of March 2014.


Notary Public, State of Wisconsin
My commission expires permanent.


Charles Sadler, Jr., Notary Public
White Twp., Indiana County
My Commission Expires June 2, 2015